Remarks

The above Amendments, these Remarks, and the Request for Continued Examination are in reply to the Office Action mailed April 18, 2007, the Examiner Interview of July 20, 2007, and the Examiner Interview Summary mailed August 9, 2007.

I. Summary of Examiner's Rejections

Claims 1, 2, 4-13, 15-19, 21-30, 32-34, and 40 were pending in the Application prior to the outstanding Office Action. In the Office Action, the Examiner rejected claims 1, 2, 4-13, 15-19, 21-30, 32-34, and 40.

Claims 1 and 18 were objected to because of informalities.

Claims 1, 2, 4-13, 15-19, 21-30, 32-34, and 40 were rejected under 35 U.S.C. 112 as allegedly being indefinite.

Claims 1, 13, 15-18, 30, and 32-34 were rejected under 35 U.S.C. 102(e) as anticipated by Sampson (U.S. Patent No. 6,339,423), or in the alternative, under 35 U.S.C. 103(a) as obvious over Sampson in view of Sharma (U.S. Patent No. 7, 089,584).

Claims 2, 4, 13, 15-16, 19, 21, 30, and 32-33 were rejected under 35 U.S.C. 103(a) as obvious over Sampson in view of Sharma.

Claims 5-11, 22-28, and 40 were rejected under 35 U.S.C. 103(a) as obvious over Sampson in view of Sharma and further in view of Hummel (U.S. Patent No. 6,584,454).

II. Summary of Applicant's Response

This Request for Continued Examination amends claims 1, 5-7, 10-12, 18, 22-24, and 27-29,

cancels claims 8, 9, 13, 15-17, 25, 26, 30, 32-34, and 40, and adds new claims 42-43, leaving for the Examiner's present consideration claims 1-2, 4-7, 10-12, 18-19, 21-24, 27-29, and 42-43. The claims were amended to better define embodiments of Applicant's invention. Reconsideration of the claims is requested.

III. Summary of Examiner Interview of July 20, 2007

Applicant acknowledges with thanks Examiner Pich's assistance in granting an interview on July 20, 2007, during the course of which interview various features of the claimed embodiments were discussed, the substance of which is included herein. The Interview Summary mailed August 9, 2007 accurately lists the topics discussed during the interview.

IV. Response to Objections to Claims 1 and 18

The amendments to the Claims have rendered the objections moot.

V. Response to 35 U.S.C. 112 Rejections to Claims 1-2, 4-7, 10-12, 18-19, 21-24, and 27-29

The amendments to the Claims have rendered the 35 U.S.C. 112 Rejections moot.

VI. Response to 35 U.S.C. 102(e) Rejections to Claims 1 and 18

Claim 1

Claim 1 (as amended) states:

> A security system for allowing a client to access a protected resource through an application container, the security system comprising:
> an application container, which provides services for a protected resource, wherein the application container delegates authorization decisions to a security service

by passing an access request and a callback handler to the security service when the application container receives the access request for a protected resource from a client;

context information, wherein the context information comprises one or more parameter values describing the access request, identity of the protected resource, and profile information describing the client;

the security service for making a decision to permit or deny the access request, wherein a plurality of security plug-ins that implement an access decision interface are plugged into the security service, and wherein the plurality of security plug-ins use the callback handler to request context information from the application container for the access request, and wherein the plurality of security plug-ins determine roles for which the client is entitled, and wherein association of the client to roles can be computed dynamically at runtime, and wherein depending on output from each security plug-in the security service determines entitlements for the client to use with the protected resource; and

the security service is located at a first computer, and the protected resource is located either at the first computer or at a second computer.

The Office Action alleges that Sampson discloses the features of Claim 1. Sampson teaches a security system that provides access to resources in multiple domains. While Sampson is in the field of internet security, applicant respectfully submits that there are significant differences between the features of Claim 1 and Sampson.

Claim 1 (as amended) requires the plurality of security plug-ins determining roles for which the client is entitled, and wherein association of the client to roles can be computed dynamically at runtime. Sampson does not disclose having the plurality of security plug-ins determine roles for which the client is entitled, and wherein association of the client to roles can be computed dynamically at runtime. Association of the client to roles being computed dynamically at runtime is not mentioned in Sampson. Paragraph 9 of Applicant's specification explains that role-based access control, as defined in the J2EE specification, is static and not dynamic.

Claim 1 requires that a plurality of security plug-ins use the callback handler to request context information from the application container. The Office Action argues that Sampson reads

upon this feature, arguing that causing a browser to redirect is the equivalent of a plurality of security plug-ins use the callback handler to request context information from the application container. As Sampson explains in col. 7, line 25, "the term redirect refers to transmitting a redirection to a browser, which is data that causes the browser to generate another request to access another resource specified in the redirection." Causing a browser to redirect is not the equivalent of or otherwise disclose a plurality of security plug-ins use the callback handler to request context information from the application container. During the examiner interview, the examiner suggested that the callback handler could be broadly interpreted to cover Sampson's browser redirect and that the security plug-ins could be broadly interpreted to cover several servers in Sampson's architecture. Yet the resulting hypothetical system as constructed by the Office Action would not have the plurality of security plug-ins using the callback handler to request context information from the application container.

Applicant respectfully submits that the embodiment as defined in Independent Claim 1 is not anticipated by Sampson. Applicant respectfully requests that the 35 U.S.C. § 102(e) rejection to Claim 1 be withdrawn.

Claim 18

Claim 18 (as amended) states:

> A method of allowing a client to access a protected resource through an Application Container, the method comprising:
> receiving at an application container, which provides services to the resources it contains, an access request from the client to access the protected resource;
> communicating the access request from the application container to a security service with the access request and a callback handler, wherein the application container delegates authorization decisions to the security service by passing an access

request and a callback handler to the security service when the application container receives an access request for the protected resource from a client;

making a decision at the security service to permit or deny the access request, wherein a plurality of security plug-ins that implement an access decision interface are plugged into the security service;

using the callback handler at each security plug-in to request context information from the application container for the access request, wherein the context information comprises one or more parameter values describing the access request, identity of the protected resource, and profile information describing the client;

determining entitlements for the client to use with the protected resource depending on output from each security plug-in, wherein the plurality of security plug-ins determine roles for which the client is entitled, and wherein the association of the client to roles can be computed dynamically at runtime; and

communicating a permitted access request to the protected resource.

The Office Action alleges that Sampson discloses the features of Claim 18. Sampson teaches a security system that provides access to resources in multiple domains. While Sampson is in the field of internet security, applicant respectfully submits that there are significant differences between the features of Claim 18 and Sampson.

Claim 18 (as amended) requires the plurality of security plug-ins determining roles for which the client is entitled, and wherein association of the client to roles can be computed dynamically at runtime. Sampson does not disclose having the plurality of security plug-ins determine roles for which the client is entitled, and wherein association of the client to roles can be computed dynamically at runtime. Association of the client to roles being computed dynamically at runtime is not mentioned in Sampson. Paragraph 9 of Applicant's specification explains that role-based access control, as defined in the J2EE specification, is static and not dynamic.

Claim 18 requires that a plurality of security plug-ins use the callback handler to request context information from the application container. The Office Action argues that Sampson reads upon this feature, arguing that causing a browser to redirect is the equivalent of a plurality of

security plug-ins use the callback handler to request context information from the application container. As Sampson explains in col. 7, line 25, "the term redirect refers to transmitting a redirection to a browser, which is data that causes the browser to generate another request to access another resource specified in the redirection." Causing a browser to redirect is not the equivalent of or otherwise disclose a plurality of security plug-ins use the callback handler to request context information from the application container. During the examiner interview, the examiner suggested that the callback handler could be broadly interpreted to cover Sampson's browser redirect and that the security plug-ins could be broadly interpreted to cover several servers in Sampson's architecture. Yet the resulting hypothetical system as constructed by the Office Action would not have the plurality of security plug-ins using the callback handler to request context information from the application container.

Applicant respectfully submits that the embodiment as defined in Independent Claim 18 is not anticipated by Sampson. Applicant respectfully requests that the 35 U.S.C. § 102(e) rejection to Claim 18 be withdrawn.

VII. Response to 35 U.S.C. 103(a) Rejections to Claims 1-2, 4-7, 10-12, 18-19, 21-24, and 27-29

Claim 1

Claim 1 (as amended) states:

> A security system for allowing a client to access a protected resource through an application container, the security system comprising:
> an application container, which provides services for a protected resource, wherein the application container delegates authorization decisions to a security service by passing an access request and a callback handler to the security service when the application container receives the access request for a protected resource from a client;

context information, wherein the context information comprises one or more parameter values describing the access request, identity of the protected resource, and profile information describing the client;

the security service for making a decision to permit or deny the access request, wherein a plurality of security plug-ins that implement an access decision interface are plugged into the security service, and wherein the plurality of security plug-ins use the callback handler to request context information from the application container for the access request, and wherein the plurality of security plug-ins determine roles for which the client is entitled, and wherein association of the client to roles can be computed dynamically at runtime, and wherein depending on output from each security plug-in the security service determines entitlements for the client to use with the protected resource; and

the security service is located at a first computer, and the protected resource is located either at the first computer or at a second computer.

The Office Action alleges that the combination of Sampson and Sharma suggests the features of Claim 1. Sampson teaches a security system that provides access to resources in multiple domains. Sharma discloses security architecture for integration of Enterprise Information Systems with J2EE. While both Sampson and Sharma are in the field of internet security, applicant respectfully submits that there are significant differences between the features of Claim 1 and the cited documents.

Claim 1 (as amended) requires the plurality of security plug-ins determining roles for which the client is entitled, and wherein association of the client to roles can be computed dynamically at runtime. Sampson and Sharma do not suggest having the plurality of security plug-ins determine roles for which the client is entitled, and wherein association of the client to roles can be computed dynamically at runtime. Association of the client to roles being computed dynamically at runtime is not suggested in either Sampson or Sharma or the combination of the two. Paragraph 9 of Applicant's specification explains that role-based access control, as defined in the J2EE specification, is static and not dynamic.

The Office Action cites the combination of Sharma's callback handler with Sampson's teachings to disclose Claim 1's requirement of a plurality of security plug-ins use the callback handler to request context information from the application container. During the examiner interview, the examiner suggested that the security plug-ins could be broadly interpreted to cover several servers in Sampson's architecture. Yet the resulting hypothetical system as constructed by the Office Action would not have the plurality of security plug-ins using the callback handler to request context information from the application container.

Applicant respectfully submits that the embodiment as defined in Independent Claim 1 is not obvious in view of the combination of Sampson and Sharma. Applicant respectfully requests that the 35 U.S.C. § 103(a) rejections to claim 1 be withdrawn.

Claim 5

The Office Action alleges that Claim 5's requirement that each of the plurality of security plug-ins can determine a contributory decision to permit, deny, or abstain from the access request is disclosed by Hummel (col 3, lines 4-20). However, the cited portion of Hummel, when combined with Sampson and Sharma, would not result in Applicant's invention as claimed. In Hummel, an agency module intercepts requests for access and contacts a policy server for authenticating passwords. Security codes are authenticated by a security server. Hummel's system divides up tasks amongst different components, Hummel's system does not provide contributory decision-making wherein each security plug-in determines a permit, deny, or abstain for an access request. Furthermore, there is no discussion or suggestion of abstaining from security decisions in Hummel. Hummel does not have a plurality of security plug-ins, instead Hummel only has the policy server.

Claim 6

The Office Action alleges that Hummel (col . 3, lines 39-60) discloses Claim 6's requirement that the security server further includes an access controller for transferring the access request to the plurality of security plug-ins, and for combining the contributory decisions into an overall decision by the security service to permit or deny the access request. However, the cited portion of Hummel, when combined with Sampson and Sharma, would not result in Applicant's invention as claimed. In Hummel, some users have a two-factor security clearance, and must enter both a password and a security code for access. In Hummel, the password is authenticated by a policy server and the security code is authenticated by a security server. Hummel has two authentication systems for high-level protected applications, but there is no disclosure or suggestion of combining contributory decisions into an overall decision to permit or deny the access request. Hummel does not have a plurality of security plug-ins, instead it only has the policy server.

Claim 7

The Office Action alleges that Hummel (col 3, lines 50-60) suggests wherein one or more of the plurality of the security plug-ins represent a business function related access policy. Hummel does not have a plurality of security plug-ins, instead it only has the policy server.

Claim 10

The Office Action alleges that Hummel (col. 12, lines 25-32) suggests wherein a deny or abstain by any one of the plurality of security plug-ins causes the security service to deny the access

request. The cited portion of Hummel does not disclose or suggest a security plug-in that can abstain from making a decision. Furthermore, the cited portion of Hummel does not disclose or suggest a plurality of security plug-ins, instead Hummel teaches a security server that authenticates a security code and then forwards the results of the authentication to a policy server.

Claim 11

The Office Action alleges that Hummel (col. 3, lines 6-11) suggests wherein an abstain by any one of the plurality of security plug-ins does not cause the security service to deny the access request. The cited portion of Hummel does not suggest a security plug-in that can abstain from making a decision. The Office Action alleges that if the resource/application is open, then the agency module makes a decision to allow access while the policy server is not consulted about the access thereby abstaining from a decision. The Office Action is alleging that if the user is requesting access to an open or unsecured resource, a resource not protected by the policy server, that when the agency module forwards the access request to the web server, that the policy server has somehow abstained from the access decision. In these circumstances, according to Hummel, the policy server is not consulted. Under Hummel, there is no abstaining, the policy server is never asked for a decision.

Claims 2, 4-7, 10-12, and 42

Dependent Claims 2, 4-7, 10-12, and 42 depend from Claim 1. For at least the reasons discussed above, Dependent Claims 2, 4-7, 10-12, and 42 are patentable. Dependent Claims 2, 4-7, 10-12, and 42 add their own features which render them patentable in their own right.

Claim 18

Claim 18 (as amended) states:

A method of allowing a client to access a protected resource through an Application Container, the method comprising:

receiving at an application container, which provides services to the resources it contains, an access request from the client to access the protected resource;

communicating the access request from the application container to a security service with the access request and a callback handler, wherein the application container delegates authorization decisions to the security service by passing an access request and a callback handler to the security service when the application container receives an access request for the protected resource from a client;

making a decision at the security service to permit or deny the access request, wherein a plurality of security plug-ins that implement an access decision interface are plugged into the security service;

using the callback handler at each security plug-in to request context information from the application container for the access request, wherein the context information comprises one or more parameter values describing the access request, identity of the protected resource, and profile information describing the client;

determining entitlements for the client to use with the protected resource depending on output from each security plug-in, wherein the plurality of security plug-ins determine roles for which the client is entitled, and wherein the association of the client to roles can be computed dynamically at runtime; and

communicating a permitted access request to the protected resource.

The Office Action alleges that the combination of Sampson and Sharma suggests the features of Claim 18. Sampson teaches a security system that provides access to resources in multiple domains. Sharma discloses security architecture for integration of Enterprise Information Systems with J2EE. While both Sampson and Sharma are in the field of internet security, applicant respectfully submits that there are significant differences between the features of Claim 18 and the cited documents.

Claim 18 (as amended) requires the plurality of security plug-ins determining roles for which the client is entitled, and wherein association of the client to roles can be computed dynamically at

runtime. Sampson and Sharma do not suggest having the plurality of security plug-ins determine roles for which the client is entitled, and wherein association of the client to roles can be computed dynamically at runtime. Association of the client to roles being computed dynamically at runtime is not suggested in either Sampson or Sharma or the combination of the two. Paragraph 9 of Applicant's specification explains that role-based access control, as defined in the J2EE specification, is static and not dynamic.

The Office Action cites the combination of Sharma's callback handler with Sampson's teachings to disclose Claim 18's requirement of a plurality of security plug-ins use the callback handler to request context information from the application container. During the examiner interview, the examiner suggested that the security plug-ins could be broadly interpreted to cover several servers in Sampson's architecture. Yet the resulting hypothetical system as constructed by the Office Action would not have the plurality of security plug-ins using the callback handler to request context information from the application container.

Applicant respectfully submits that the embodiment as defined in Independent Claim 18 is not obvious in view of the combination of Sampson and Sharma. Applicant respectfully requests that the 35 U.S.C. § 103(a) rejections to claim 18 be withdrawn.

Claim 22

The Office Action alleges that Claim 22's requirement that each of the plurality of security plug-ins can determine a contributory decision to permit, deny, or abstain from the access request is suggested by Hummel (col. 3, lines 4-20). However, the cited portion of Hummel, when combined with Sampson and Sharma, would not result in Applicant's invention as claimed. In Hummel, an

agency module intercepts requests for access and contacts a policy server for authenticating passwords. Security codes are authenticated by a security server. Hummel's system divides up tasks amongst different components, Hummel's system does not provide contributory decision-making wherein each security plug-in determines a permit, deny, or abstain for an access request. Furthermore, there is no discussion or suggestion of abstaining from security decisions in Hummel. Hummel does not have a plurality of security plug-ins, instead Hummel only has the policy server.

Claim 23

The Office Action alleges that Hummel (col. 3, lines 39-60) suggests Claim 23's requirement that the security server further includes an access controller for transferring the access request to the plurality of security plug-ins, and for combining the contributory decisions into an overall decision by the security service to permit or deny the access request. However, the cited portion of Hummel, when combined with Sampson and Sharma, would not result in Applicant's invention as claimed. In Hummel, some users have a two-factor security clearance, and must enter both a password and a security code for access. In Hummel, the password is authenticated by a policy server and the security code is authenticated by a security server. Hummel has two authentication systems for high-level protected applications, but there is no disclosure of combining contributory decisions into an overall decision to permit or deny the access request. Hummel does not have a plurality of security plug-ins, instead it only has the policy server.

Claim 24

The Office Action alleges that Hummel (col. 3, lines 50-60) suggests wherein one or more of

the plurality of the security plug-ins represent a business function related access policy. Hummel does not have a plurality of security plug-ins, instead it only has the policy server.

Claim 27

The Office Action alleges that Hummel (col. 12, lines 25-32) disclose wherein a deny or abstain by any one of the plurality of security plug-ins causes the security service to deny the access request. The cited portion of Hummel does not suggest a security plug-in that can abstain from making a decision. Furthermore, the cited portion of Hummel does not disclose or suggest a plurality of security plug-ins, instead Hummel teaches a security server that authenticates a security code and then forwards the results of the authentication to a policy server.

Claim 28

The Office Action alleges that Hummel (col. 3, lines 6-11) suggests wherein an abstain by any one of the plurality of security plug-ins does not cause the security service to deny the access request. The cited portion of Hummel does not suggest a security plug-in that can abstain from making a decision. The Office Action alleges that if the resource/application is open, then the agency module makes a decision to allow access while the policy server is not consulted about the access thereby abstaining from a decision. The Office Action is alleging that if the user is requesting access to an open or unsecured resource, a resource not protected by the policy server, that when the agency module forwards the access request to the web server, that the policy server has somehow abstained from the access decision. In these circumstances, according to Hummel, the policy server is not consulted. Under Hummel, there is no abstaining, the policy server was never asked for a

decision.

Claims 19, 21-24, 27-29, and 43

Dependent Claims 19, 21-24, 27-29, and 43 depend from Claim 18. For at least the reasons discussed above, Dependent Claims19, 21-24, 27-29, and 43 are patentable. Dependent Claims 19, 21-24, 27-29, and 43 add their own features which render them patentable in their own right.

VIII. Conclusion

In light of the above, it is respectfully submitted that all of the claims now pending in the subject patent application should be allowable, and a Notice of Allowance is requested. The Examiner is respectfully requested to telephone the undersigned if he can assist in any way in expediting issuance of a patent.

Enclosed is a PETITION FOR EXTENSION OF TIME UNDER 37 C.F.R. §1.136 for extending the time to respond up to and including today, August 20, 2007.

The Commissioner is authorized to charge any underpayment or credit any overpayment to Deposit Account No. 06-1325 for any matter in connection with this response, including any fee for extension of time, which may be required.

Respectfully submitted,

Date: August 20, 2007

By: /Thomas K. Plunkett/
Thomas K. Plunkett
Reg. No. 57,253

Customer No. 23910
FLIESLER MEYER LLP
650 California Street, Fourteenth Floor
San Francisco, California 94108
Telephone: (415) 362-3800